Applied Quantitative Analysis, Vol. 6 No. 2 (2026) https://doi.org/10.31098/quant.4555

Check for updates

Research Paper

A Lightweight BYOD Cybersecurity Governance and Risk Assessment Framework for University Students

B.N. Paridya*, E.D.K. Chamara, H.I.K. Jayarathna, P.H. Haputhanthri, R.B.S.H. Gunasekara, K.M. Piyumal

University of Kelaniya, Sri Lanka

Received : June 13, 2026	Revised : August 14, 2026	Accepted : August 14, 2026	Online : August 21, 2026

Abstract

The increasing use of personal laptops, smartphones, and tablets for academic activities has made Bring Your Own Device (BYOD) practices common in university environments. Although BYOD improves flexibility and accessibility, it also creates cybersecurity and data protection risks, including weak password practices, outdated devices, unsafe network usage, malware exposure, and limited user awareness. This study aims to develop a lightweight BYOD cybersecurity governance and risk assessment framework for university students. A quantitative survey-based method is used to collect data from university students regarding their BYOD usage and security practices. The collected responses are analyzed using descriptive statistics and a likelihood-impact risk scoring model. Based on the findings, the study proposes the Lightweight BYOD Governance and Risk Framework, which includes risk identification, risk assessment, governance, protection, education, and periodic review. The proposed framework provides practical guidance for universities to manage BYOD-related risks using simple and low-cost governance controls. The study contributes to cybersecurity governance by connecting student behavior, risk assessment, and policy-based security recommendations in a university context.

Keywords: *BYOD, Cybersecurity Governance, Risk Assessment, University Students, Information Security, NIST CSF, ISO/IEC 27001, Data Protection*

INTRODUCTION

Digital transformation of higher education (Batalla et al., 2026) has increased the use of personal digital devices for academic activities. University students commonly use personal laptops, smartphones, and tablets to access learning management systems, online lectures, academic email, and student information systems (Dina, 2025). This is called Bring Your Own Device (BYOD). BYOD improves flexibility, accessibility, mobility, and convenience, allowing students to continue academic activities beyond the classroom using their own devices.

However, despite its advantages, BYOD introduces significant cybersecurity and data protection risks (Barruga, 2025). Unlike institution-managed devices, student-owned devices are generally outside the university's control and may not follow standard security requirements. Weak passwords, password reuse, installation of malicious software, insecure public Wi-Fi usage, lack of physical security controls, untrusted applications, and limited cybersecurity awareness (Weeratunge et al., 2026) may expose both students and universities to cyber threats (Soni et al., 2026), such as phishing (Althobaiti et al., 2024), credential theft, malware infection, unauthorized access, and data leakage (Bwiino et al., 2026).

Literature Survey

Previous studies have stated the security risks of BYOD and the necessity of implementing policies to mitigate those risks (Harthy, 2022). Other studies have emphasized that weak passwords, password reuse, and poor awareness significantly increase cybersecurity exposure in

Corresponding author's email: paridya-ct20061@stu.kln.ac.lk

educational environments (Bottyan, 2023).

Research related to cybersecurity awareness (Ajmal, 2026) has shown that human behavior (Essahraui et al., 2025) remains one of the major cybersecurity risk factors (Kepuska & Tomasevic, 2024). Even when technical security controls (Yaakub et al., 2026) exist, unsafe user behavior—such as reusing passwords, failing to enable multi-factor authentication, and clicking suspicious links—can still lead to security incidents, including credential stuffing, brute-force exploits, social engineering, and targeted phishing campaigns (Whitman & Mattord, 2021).

Previous research has also highlighted the importance of combining policy and compliance, risk management (Akampurira et al., 2026), monitoring and review, incident response and recovery, and user awareness in higher education environments (Ali, 2025). However, a research gap remains: limited research has integrated student cybersecurity behavior, simplified risk scoring, governance recommendations, and framework-based controls into one lightweight model specifically designed for university environments.

To address this limitation, this study aims to develop a lightweight BYOD cybersecurity governance and risk assessment framework for university environments. The proposed framework has four core pillars:

1. Risk Identification
2. Behavioral Analysis
3. Low-Overhead Risk Assessment
4. Governance-Oriented (Moeti et al., 2025) Countermeasures

To achieve this, the study adopts a survey-based research methodology to analyze current cybersecurity practices and behavioral patterns among university students. The scientific contribution of this research lies in the development of a Lightweight BYOD Governance and Risk Framework (L-BGRF) specifically designed for university environments. Unlike previous studies that focus only on awareness, policy compliance, or technical security controls, the proposed framework combines:

1. Student cybersecurity behavior analysis
2. BYOD risk identification
3. Simplified risk scoring
4. Governance-oriented recommendations
5. Awareness improvement strategies
6. Framework-based control mapping

Research Objectives

1. To identify common cybersecurity risks (Handri et al., 2026) associated with students' devices in university environments.
2. To examine student cybersecurity practices related to passwords, software updates, antivirus usage, public Wi-Fi usage, multi-factor authentication, and data backup practices.
3. To assess BYOD cybersecurity risks using a lightweight likelihood-impact risk scoring model.
4. To map governance-oriented BYOD security recommendations to NIST CSF 2.0 and ISO/IEC 27001 principles (Vasović et al., 2026).
5. To propose a lightweight BYOD governance and risk framework for university environments.

LITERATURE REVIEW

Pioneering studies Abdul Halim et al., 2024 focus on the infrastructure security threats posed

by unmanaged endpoints. The study focuses on identifying the necessary components that could assist top management and policymakers in developing a BYOD security policy. The study analyses 2013 to 2022 BYOD security policy-related articles from 2013 to 2022. The study has developed a BYOD security policy based on these existing policy frameworks. The framework does not describe the implementation of the proposed BYOD security policy.

Kepuska & Tomasevic, 2024 demonstrate a lightweight framework for cyber risk management in Western Balkan higher education institutions. The framework focuses on identifying vulnerabilities in learning management systems (LMS) in Western Balkan countries and suggests proactive controls based on a penetration testing approach. The proposed framework consists of three layers: a strategic layer, an operational layer, and an implementation layer. The strategic layer consists of Penetration testing objectives (PTOs), Tactics, Techniques, Tools, and Procedures, Vulnerability management, and Proactive controls. The operational layer consists of Penetration testing steps, TTTP frameworks, and different control types. The implementation layer consists of offensive and defensive strategies. The study used eight HEIs in the Western Balkans and identified 20 vulnerabilities using the proposed framework. The results show that, among these vulnerabilities, Fingerprint WebServer and SSL version 2 support are identified as the most common vulnerabilities in most of the HEIs. The solution is only based on LMS-based vulnerabilities, not on student behavior-based vulnerabilities. Critical synthesis of these two domains reveals a significant mismatch: technical perimeters are ineffective if student behavioral vulnerabilities are present.

Harthy, 2022 proposed a risk management and security framework to detect and predict risks using Mobile Device Management (MDM) event logs and function logs. The study also examines the level of user awareness of BYOD security methods. The proposed framework can predict and identify security risks and then provide prevention plans. Users of this framework must install the MDM agent and connect to organizational resources via the MDM agent; then, the MDM administrator applies access controls using the employee's category and rules. The framework classifies the log records using machine-learning algorithms and flags events as normal or abnormal. The SVM algorithm achieved the highest accuracy of 96%. However, the solution is limited to mobile devices.

Dina, 2025 introduces a study to evaluate the risks associated with BYOD integration regarding security vulnerabilities in South African higher education Learning Management Systems (LMSs). The study focuses on the security awareness of users with a higher education institute's LMS. It examines the users' perception of cybersecurity risks and whether institutional security policies effectively enhance security awareness and compliance. According to the data analysis in the study, the results show that "Unauthorized Access" is the highest occurring risk type in South African Higher Education LMSs with BYOD devices. The solution is based only on LMS system-based vulnerabilities, not on student behavior-based vulnerabilities.

Osijirin et al., 2026 proposed a solution to examine the threat landscape Hassan et al., 2025 of higher education institutions, focusing on ransomware threats, phishing attacks, and insider threats. It also focuses on data breaches and the emerging risks associated with generative artificial intelligence (Zentner et al., 2026). The study mainly focuses on technologies such as zero-trust architectures, AI-driven intrusion detection, multi-factor authentication, and cloud security frameworks. The entire document provides a comparison between existing solutions, but it does not provide any novel framework based on these existing solutions.

The proposed framework is based not only on technical factors but also on user behaviors and practices, such as the percentage of suspicious link clicks, the percentage of reuse of the same password, the percentage of Multi-factor Authentication usage, the percentage of public Wi-Fi usage, etc. The framework is also aligned with the core security standards of NIST CSF 2.0 and

ISO/IEC 27001. Therefore, the framework is not only a theoretical framework but also aligns with practical aspects, offering strong security considerations when compared to existing solutions.

Theoretical Framework: NIST CSF 2.0 and ISO/IEC 27001 Alignment

This study synthesizes principles from two preeminent international cybersecurity standards: the NIST Cybersecurity Framework (CSF) 2.0 and ISO/IEC 27001. Rather than applying these frameworks in their exhaustive, enterprise-grade formats, this research distills their core pillars to accommodate the distinct operational realities of higher education networks.

NIST CSF 2.0

The execution of this framework relies on six interdependent pillars mapped directly to the student environment (National Institute of Standards and Technology, 2024):

1. Govern (GV): The organization's cybersecurity risk management strategy, expectations, and policies are established, communicated, and monitored.
2. Identify (ID): The organization's current cybersecurity risks are understood
3. Protect (PR): Safeguards to manage the organization's cybersecurity risks are used
4. Detect (DE): Possible cybersecurity attacks and compromises are found and analyzed
5. Respond (RS): Actions regarding a detected cybersecurity incident are taken
6. Recover (RC): Assets and operations affected by a cybersecurity incident are restored

ISO/IEC 27001 and Information Security Management Systems (ISMS)

ISO/IEC 27001 provides the requirements for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS) (International Organization for Standardization [ISO], 2022). Evaluating the standard through an academic lens requires adapting its core management clauses into a lightweight model:

1. Context of the Organization: The university should determine the boundaries of a university environment that balances open academic freedom with infrastructure security.
2. Leadership: Ensuring that system policies do not unnecessarily impact the student user experience.
3. Planning: Formulating strategic security goals by mapping student-specific vulnerabilities identified through the risk assessment process to risk treatment options.
4. Support: Providing the necessary organizational resources, specifically targeting continuous security awareness campaigns.
5. Operation: Planning, implementing, and controlling the recommended risk mitigation processes at planned intervals without disrupting day-to-day academic workflows.
6. Performance Evaluation: Reviewing and measuring the effectiveness of deployed controls using internal audits and management reviews.
7. Improvement: Continually modifying the lightweight framework by improving its suitability, adequacy, and effectiveness to adapt to evolve risks and student behaviors.

Research Gap

While existing literature thoroughly addresses Bring Your Own Device (BYOD) security risks, current risk assessment models and governance frameworks are engineered primarily for corporate environments. These previous studies mainly focus on technical aspects such as LMSs, networks, and common attacks, but do not focus on user behaviors. These enterprise frameworks assume centralized IT control, large budgets, and the authority to monitor personal devices.

At the same time, a significant research gap exists regarding higher education institutions.

Universities operate as open, decentralized, and resource-constrained networks that must balance network security with academic freedom and student privacy. Current frameworks fail to address this specific environment. This study bridges the gap by introducing the Lightweight BYOD Governance and Risk Framework (L-BGRF), a model designed for the operation of a university network, including user technologies and user behaviors in higher education institutes.

RESEARCH METHOD

Research Design

This study employs a quantitative survey-based research design. An online survey method is appropriate because it focuses on student BYOD behavior, cybersecurity awareness, and security practices. The collected data will be processed using descriptive statistics and a risk scoring model.

Population and Sample

The specific population for this research includes university students who use personal devices, such as laptops, smartphones, and tablets, for academic activities. The sample includes 100 undergraduate students from the University of Kelaniya. We have used a convenience sampling method because the research was conducted within a limited academic period.

Data Collection Instrument

Data were gathered using a web-based questionnaire administered via Google Forms. The instrument consists of questions to assess two primary domains: device usage topologies and individual security compliance patterns (Dawaare, 2025), including:

1. Identity & Authentication: Device access locks, credential complexity, password reuse habits, and multi-factor authentication (MFA) adoption.
2. Endpoint Maintenance: Operating system patch management frequency and antivirus deployment.
3. Network & Data Integrity: Public Wi-Fi connection habits, personal cloud storage usage (Almarhabi et al., 2018), and data backup frequencies.
4. Threat Awareness: Susceptibility to phishing and exposure to institutional cybersecurity awareness training.

The survey link was distributed via WhatsApp over a fixed fourteen-day period. The survey questions and answer options are shown in Table 1.

Ethical Considerations

To safeguard student privacy and encourage authentic reporting of risky digital behaviors, the data collection design strictly enforces absolute anonymity. The collection instrument was configured to block the gathering of personally identifiable information (PII), including student names, identification numbers, telephone numbers, and email addresses. Furthermore, a formal disclosure statement was embedded in the introductory interface of the survey, informing participants that their participation was entirely voluntary and that all aggregated data would be processed solely for academic research purposes.

Data Analysis & Risk Scoring Method

Quantitative data analysis was performed using Microsoft Excel to compute frequency counts and percentage distributions for each behavioral indicator.

The framework uses a simplified, lightweight Likelihood-Impact matrix to calculate overall

threat levels without the heavy computational overhead of enterprise risk suites. Each identified BYOD risk is evaluated against two parameters scored on a scale from 1 to 5:

$$Risk\ Score = Likelihood * Impact$$

Where:

1. Likelihood (1–5): Higher percentages of students engaging in a risky behavior correspond to higher probability scores.
2. Impact (1–5): Derived from the technical severity of the threat vector on the university network infrastructure.

Survey Questions

Table 1. Survey Question

No.	Questions	Answer Options
1	Do you use your personal laptop or smartphone for university work?	Yes / No
2	What type of device do you mostly use for academic work?	Laptop / Smartphone / Tablet / Multiple devices
3	Do you use a strong password or PIN on your device?	Yes / No / Not sure
4	Do you reuse the same password for multiple accounts?	Yes / No / Sometimes
5	Do you use two-factor authentication for email, LMS, or cloud accounts?	Yes / No / Not sure
6	Do you regularly update your device's operating system and applications?	Yes / No / Sometimes
7	Do you use antivirus or built-in security protection?	Yes / No / Not sure
8	Do you connect to public Wi-Fi for academic work?	Yes / No / Sometimes
9	Do you store university-related files in personal cloud storage?	Yes / No / Sometimes
10	Do you regularly back up important academic files?	Yes / No / Sometimes
11	Have you ever clicked a suspicious link or attachment?	Yes / No / Not sure
12	Have you received cybersecurity awareness training from your university?	Yes / No
13	Do you know how to report a cybersecurity incident to the university?	Yes / No / Not sure
14	Do you think universities should provide a clear BYOD security policy?	Yes / No / Not sure
15	Which BYOD security control do you think is most important?	Strong password / MFA / Updates / Antivirus / Backup / Awareness training
16	Do you use any kind of screen lock method to protect your devices?	Yes / No

Source: Developed from primary survey data collected for this study

FINDINGS AND DISCUSSION

Respondent Profile

The respondents include a group of students from the University of Kelaniya. The sample was collected through convenience sampling due to research time constraints. While the sample size is too small to represent all university students, it provides useful initial insights into common

BYOD usage patterns and cybersecurity practices among students. The results are therefore interpreted as an exploratory view of student BYOD behavior and not an exhaustive description of the entire university population.

As Descriptive statistics, mostly frequencies and percentages were used to analyze the responses. This method was chosen because the study's goal is to identify patterns in the observed use of devices by students and their security behavior. The results from this section support the subsequent risk assessment process by indicating the most common categories of devices used for academic work and where governance. The results from this section support the later risk assessment process by showing which device categories are most commonly used for academic work and where governance attention should be focused. Table 2 shows that most university students are using Laptops (55%) as BYODs within the faculty premises. Table 3 indicates that most of the students are following the practice of using strong passwords (81%), but a considerable number of them (42%) are reusing these passwords. They should address the issue using Multifactor Authentication (76%). Table 4 shows that most of them update their devices regularly and are aware of antivirus solutions (68%). All of them lock their screens when they are not working with their own devices, which will prevent insider threats. Table 5 shows that most of them (82%) are using public Wi-Fi. This will result in rogue access point attacks and evil twin attacks on their own devices. Also, a considerable number of them practice clicking suspicious links (37%), which will result in hacking their own devices. Using these results, Table 6 identifies high-risk activities as Password reuse, limited MFA usage, high public Wi-Fi usage, and suspicious link clicking.

BYOD Usage Pattern

Table 2. BYOD Usage Patterns

Device Category	Column User Count	Percentage
Laptop Only	55	55%
Smartphone Only	9	9%
Laptop, Smartphone	27	27%
Laptop, Smartphone, Tablet	9	9%
Total	100	100%

Source: Developed from primary survey data collected for this study

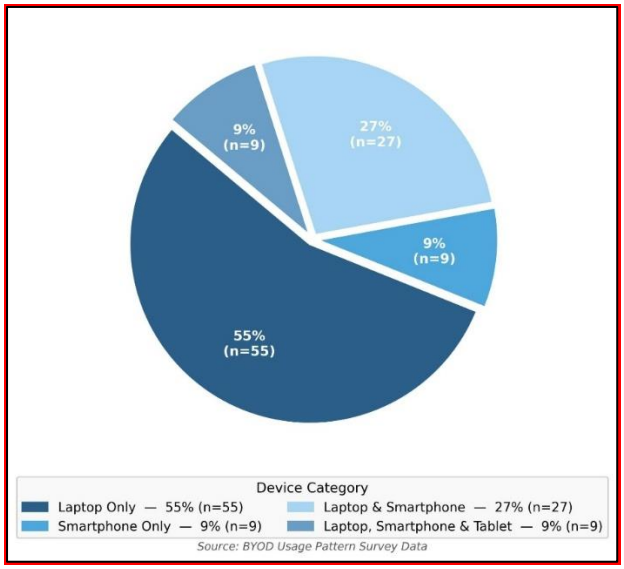

Figure 2. BYOD Usage Patterns Among Respondents

The survey results are shown in Table 2 and Figure 1. The most popular personal device used for academic work is the laptop. Out of 100 respondents, 55 students (55%) said that laptops are their main device for academic activities. This shows that laptops are still the main device for activities such as logging in to the learning (Alghabban, 2026) management system, preparing assignments, attending online sessions, working with productivity software, and storing academic documents.

9 respondents, or 9.45% of the sample, opted for smartphones as their main academic device. This percentage is lower than that of laptops, but smartphones still play an important role in the BYOD environment. Students use their smartphones for email, messaging applications, online announcements, authentication codes, file sharing, and instant access to academic resources. Therefore, smartphone security should not be ignored, even if smartphones are not the main device for most respondents.

Twenty seven respondents (27%) used both smartphones and laptop devices for academic work. This indicates that many students are not reliant on just one device; instead, they switch from a laptop to a smartphone during academic tasks. This increases the attack surface from a cybersecurity governance perspective, as each device adds another possible compromise point. For example, a student might use a laptop for assignments and a smartphone for email and cloud access. However, if one of these devices is not well protected, it can still expose academic accounts or university-related data.

No respondents reported using tablets as their main academic device. This does not mean that tablets are not used at all, as some students use multiple devices, including a laptop, a smartphone, and a tablet. It indicates that tablets are not the dominant device type in this sample. Therefore, the BYOD governance framework should mainly focus on laptops and smartphones, but remain flexible enough to incorporate other device types.

The results justify the practice of BYOD by the students surveyed. All respondents use personal devices for academic work; therefore, university cybersecurity governance cannot be limited to institutional systems such as servers, networks, and learning platforms. It should also include the security status and behavior of student-owned devices that connect to university services. This emphasizes the need for a lightweight BYOD governance and risk assessment framework to guide students without creating a security process that is too restrictive or complex.

Password and Authentication Practices

In a university BYOD environment, password and authentication practices are very important, as student accounts are frequently used to access learning management systems, emails, digital libraries, and student information systems. If a student account is compromised, attackers could gain unauthorized access to academic records, students' personal information, institutional resources, and student information. For these reasons, password strength, password reuse, and multi-factor authentication are important indicators of BYOD-related cybersecurity risk.

The results show that 81% of respondents use a strong password or PIN on their devices, while 19% either do not use a safe password or PIN, or are uncertain about the strength of their password. This is a positive finding because most students show an understanding of the basic importance of device-level access protection. However, the remaining percentage still represents a risk group because weak passwords or simple PINs can make personal devices easier to access if they are lost, stolen, or left unattended.

It seems to be a more serious problem of reusing passwords. 58% of participants exhibit safer password behavior, while 42% exhibit risky password reuse behavior. This finding is important as reused passwords amplify the impact of a single credential compromise. For example, if a student uses the same password for their personal email, university email, LMS, and cloud

storage, a single leaked password could give attackers access to multiple services. This risk is of special relevance within the BYOD context, as students tend to access several academic platforms using the same personal device.

The findings also show that 76% of respondents use multi-factor authentication. The 24% do not use MFA or are unsure if they use it. MFA is a critical security control because it adds an extra layer of verification beyond a password. If a password is compromised through phishing or leakage, MFA can help minimize the risk of unauthorized account access. The fact that nearly one-fourth of the respondents do not use MFA poses a governance issue.

The results shown in Table 3 and Figure 2 below indicate that students' password and authentication practices are moderately strong overall, but there are notable areas of risk. Strong passwords and the use of MFA are positive trends, but password reuse is a major vulnerability. In terms of governance, universities should not only advise students to create strong passwords but also advocate for the use of unique passwords, password managers, MFA activation, and phishing awareness. These controls should be included in a student-centric BYOD security policy.

Table 3. Password and Authentication Practices

Security Practice	Save Practice	Risk Practice
Strong Password/PIN	81%	19%
Password Reuse	58%	42%
MFA Usage	76%	24%

Source: Developed from primary survey data collected for this study

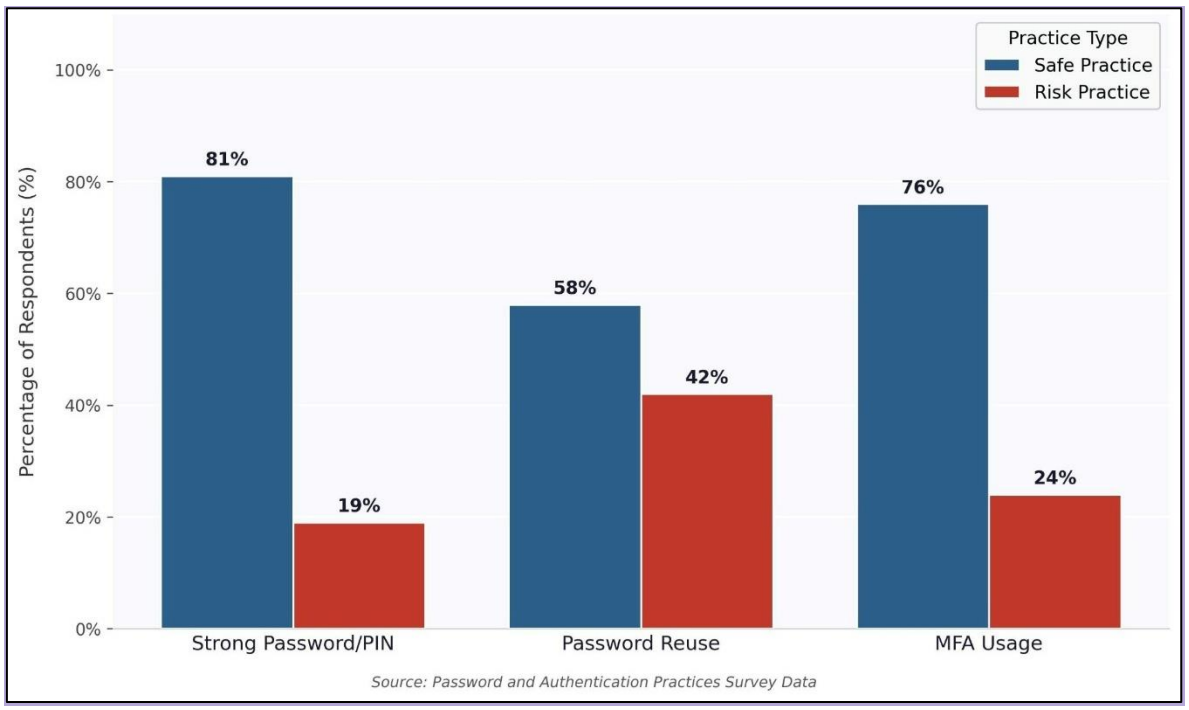

Figure 2. Password and Authentication Practices Among BYOD Users

Device Protection Practices

Table 4. Device Protection Practices

Practice	Yes	No/Sometimes
Regular Updates	68%	32%
Antivirus/Security Protection	68%	32%

Device Screen Lock	100%	0%

Source: Developed from primary survey data collected for this study

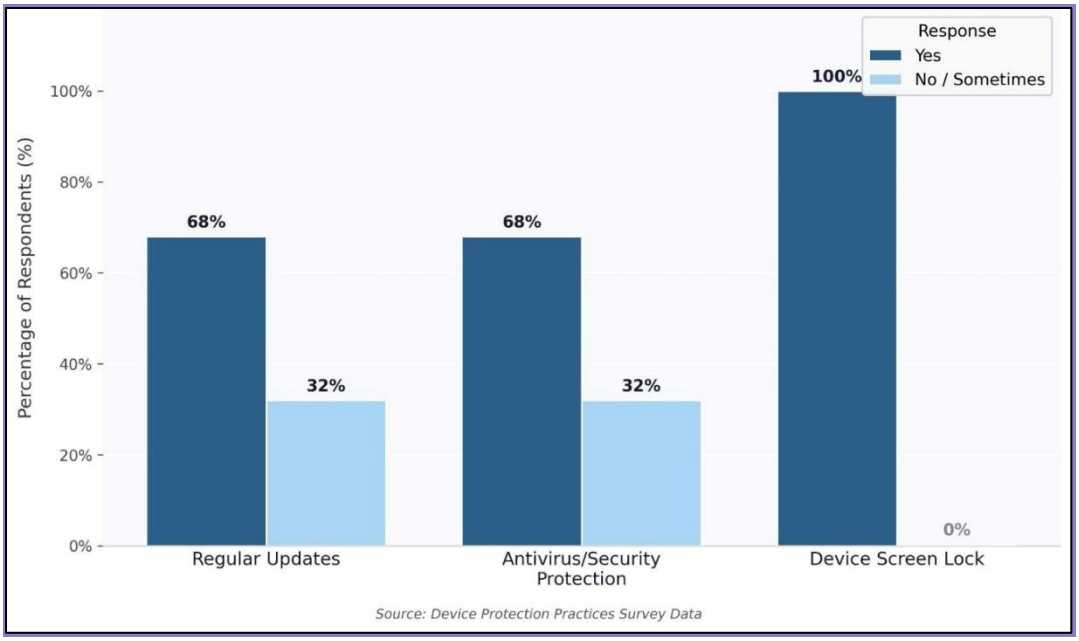

Figure 3. Device Protection Practices Among BYOD Users

Another topic that should be considered when discussing BYOD cybersecurity includes the protection of students' devices. Since students' devices are normally out of reach for the university administration and its policies, personal computers and cell phones might not be configured in line with the security standards established by universities. As a consequence, device security will depend heavily on the conduct and awareness of individual users. The results are shown in Table 4 and Figure 3 above.

The findings show that 68% of the participants perform regular updates of both the operating systems and applications installed on their devices, while 32% do not update or update only occasionally. Such results indicate a rather moderate risk, considering that outdated software can contain vulnerabilities that could be used by hackers. Updating devices is particularly important since it involves fixing bugs, reducing vulnerabilities, and updating protections.

Similarly, the usage of antivirus or security protection demonstrates the same trend. The data reveals that 68% use antivirus software, whereas 32% do not have any security measures or are unsure whether any security measures are installed on their personal devices. This shows that almost one-third of the respondents lack sufficient malware protection. This is a significant point in a BYOD environment because respondents download and install various software applications, which might lead to ransomware, malware threats, spyware, and other issues.

However, the most significant result obtained from this analysis regarding security measures taken on personal devices is the use of device screen locks. In fact, all respondents (100%) use a screen lock on their personal devices to ensure security and safety. This is a reasonable security measure, as using screen locks helps prevent unauthorized physical access to the device. Nevertheless, a screen lock is just one part of securing a personal device.

Results indicate that the use of simple visible controls is consistently practiced, while maintenance controls are not consistently adhered to by students. This may indicate that students understand basic protection methods but lack knowledge regarding the need for continual device protection. Awareness activities should, therefore, focus on both informing students with necessary

actions and the reasons for doing so. From a governance viewpoint, universities must establish minimum security requirements for student-owned BYOD. These requirements could include activating screen locks, updating devices regularly, employing antivirus software or pre-existing security features, avoiding suspicious or untrusted software, and notifying relevant parties when suspicious activity occurs on the device.

Network and Data Protection Practices

This is the case because university-related online platforms would be accessed from diverse networks, and academic data would be stored on personal devices or personal cloud accounts. Unlike university-owned devices, personal devices are usually accessed from uncontrolled networks, such as home networks, public locations, mobile networks, cafes, libraries, and other similar environments. This increases cybersecurity concerns, considering that the university has little control over the connections to its academic services. The results are shown in Table 5 and Figure 4 below.

Table 5. Network and Data Protection Practices

Practice	Save Practice	Risk Practice
Public Wi-Fi Usage	82%	18%
Personal Cloud Storage	45%	55%
No backup	79%	21%
Clicked Suspicious Links	37%	63%

Source: Developed from primary survey data collected for this study

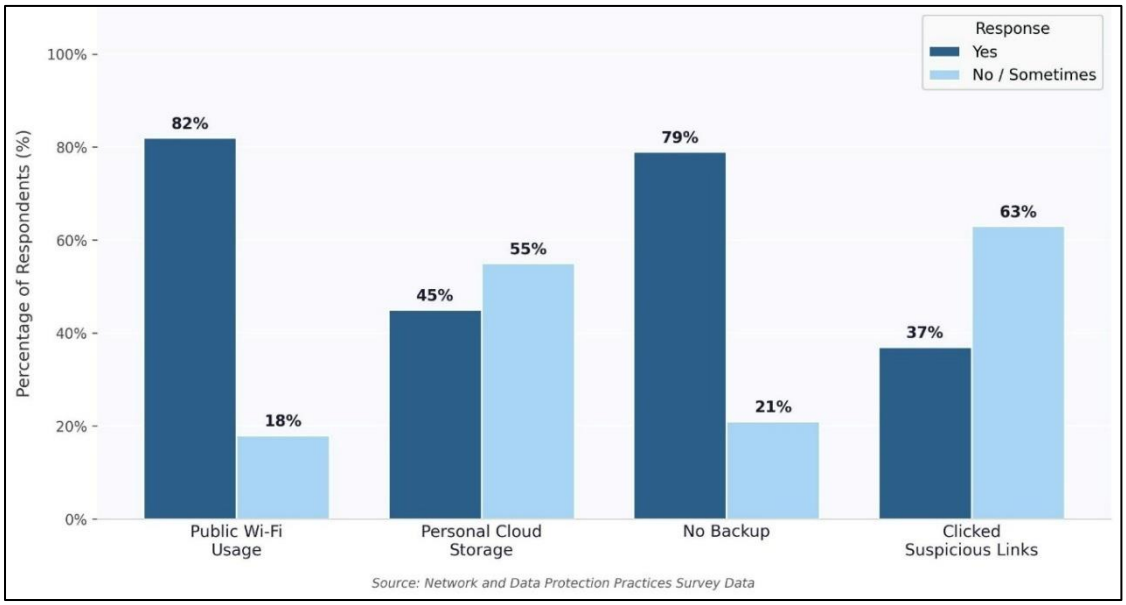

Figure 4. Network and Data Protection Practices Among BYOD Users

One of the major network-based risks identified in the survey involves the use of public Wi-Fi networks by students. According to the risk assessment results, 82% of the respondents indicated that they access university-related academic services via public Wi-Fi networks. This poses risks since public Wi-Fi networks do not always provide adequate security measures. Therefore, credential interception, spoofing of the Wi-Fi network, session hijacking, and phishing could occur when accessing a public Wi-Fi network.

Another medium risk was identified regarding personal cloud storage services, which some students used for storing and sharing their academic files using Google Drive, OneDrive, Dropbox,

or personal email accounts. While personal cloud storage solutions increase efficiency and facilitate cooperation, there can be significant concerns relating to data leakage, as files may fall into the wrong hands or lack adequate access restrictions. Furthermore, this situation may become even more critical when one considers that academic documents may also include personal data, assignments, project work, etc.

Data backups were found to pose significant security threats, as 21% of participants admitted that they sometimes do not back up their data. The absence of data backup practices presents a security risk for students' academic work, as they may experience the loss of academic data if their device is damaged, lost, stolen, attacked by viruses, or accidentally reformatted. In the BYOD context, students must ensure that they perform backups themselves.

Phishing is one of the most common ways attackers compromise student accounts. The fact that 63% of students have clicked or are unsure about clicking on a suspicious link indicates a lack of cybersecurity awareness among them. Students frequently receive links through email, messaging applications, online classrooms, social media groups, and file-sharing platforms. If students click on malicious links, they may expose login credentials, download malware, or provide sensitive information to fake websites. This risk is strongly connected to awareness, because technical controls (De La Torre et al., 2026) alone cannot fully prevent unsafe user decisions.

Risk Assessment Results

$$Risk\ Score = Likelihood * Impact$$

Risk Levels: High 15 – 25; Medium 8 – 14; Low 1 – 7

The risk assessment scores have been generated from survey results and a lightweight scoring technique that considers the likelihood and impact of risks. Likelihood refers to the frequency of occurrence of the risky behaviors observed among the subjects, whereas impact refers to the severity of the consequences that might occur when a risk materializes. Likelihood and impact were then multiplied to obtain the overall risk score. This approach was chosen due to its simplicity and effectiveness in university settings, where more sophisticated methods for enterprise-level risk assessments would not be appropriate.

From the table below, among all the risks assessed, password reuse was observed to exhibit the highest risk level. It was scored 20, indicating a high risk level. While some respondents employ strong passwords or PIN codes, reusing the same password presents a critical vulnerability. If one password is compromised via phishing attacks or a data breach, hackers can attempt to exploit that password to access other accounts, including university emails, online learning management systems (LMS), cloud storage services, and personal accounts. Hence, the impact of password reuse is greater than that of weak device access protection alone.

Table 6. Risk Assessment Results

Risk	Evidence from the Survey	Likelihood	Impact	Score	Level
Weak passwords	19% with weak passwords	3	4	12	Medium
Password reuse	42% reuse passwords	4	5	20	High
MFA	24% do not use MFA	4	4	16	High
No updates	32% do not regularly update	3	4	12	Medium
Antivirus	32% do not have or are not aware of antivirus software	3	4	12	Medium
Device screen	Every student has a screen lock.	1	2	2	Law

lock					
Public Wi-Fi	82% use public Wi-Fi	4	4	16	High
Personal cloud storage	45% use personal cloud storage	4	3	12	Medium
Backup	21% do not back up files	3	3	9	Medium
Suspicious links	37% clicked on suspicious links	4	5	20	High

Source: Developed from primary survey data collected for this study

The second risk category, with a high score of 16, relates to the lack of multi-factor authentication. Based on the survey results, only 24.32% of students use MFA or are unsure about using it. Despite being a smaller percentage of the total risks, the severity of impact remains high since multi-factor authentication provides the most efficient way to protect user accounts from breaches. Therefore, without MFA, a stolen password will grant a hacker access to a student's account. Hence, the implementation of MFA is a key part of governance in the proposed BYOD policy.

Another risk category to pay attention to received the highest score of 16. It relates to the use of public Wi-Fi by students. In this case, the risk is high in 81.08% of students stated that they use public Wi-Fi. The problem with public Wi-Fi networks is that they are not owned by universities and are therefore vulnerable to a number of attacks, such as fake access points, credential interception, session hijacking, and phishing redirection.

Irregular software updates have been rated as a medium risk based on a score of 12. The survey indicates that 32.43% of respondents do not regularly update their devices. This risk is considered medium rather than high because it depends on many factors, such as types of vulnerabilities, exposure to malicious links, and security controls.

Lastly, we consider the lack of regular backups as another medium risk (score 9). A lack of regular backups will not necessarily lead to a risk of unauthorized access; however, it can have adverse implications for data availability and academic activities. If students do not regularly back up academic data, they may lose assignments, projects, research, or study material if their devices are stolen, damaged, or attacked by malicious software.

The results are shown in Table 6. Based on the above risk assessment, it is clear that the immediate governance problems requiring attention involve password reuse, the lack of multi-factor authentication, and the use of public Wi-Fi. This is mainly because these three issues pose direct threats through credential theft, unauthorized access, and the disclosure of university information. Medium risks, such as update irregularity and the lack of backups, should be mitigated via awareness and BYOD minimum security practices.

Overview of L-BGRF

Based on literature reviews, survey results, and risk assessments, this study presents the Lightweight BYOD Governance and Risk Framework, henceforth referred to as L-BGRF. The framework targets university settings where students often use personal laptops, mobile phones, and other personal gadgets to conduct their studies. The L-BGRF does not require full control over personal devices, as is expected from corporate BYOD policy frameworks. It provides a pragmatic yet cost-effective governance framework that can be used by the students themselves. The framework components are shown in Table 7 below.

The proposed framework directly addresses the major risks discussed in this study, including reuse of passwords, lack of multi-factor authentication, connection to public networks, infrequent software updates, and inadequate data backups. All the risks presented have been associated with behaviors exhibited by the students. As such, the framework will take a governance-centered, risk-

oriented approach focused on minimum security levels and regular reviews.

The proposed framework is composed of six core elements: Identify, Assess, Govern, Protect, Educate, and Review. The framework forms a continuous cycle for managing BYOD cybersecurity risks within universities. Under the Identify element, the university determines the ways through which students use personal devices. Thereafter, a simple risk assessment using a likelihood-impact approach is conducted.

Students are provided with education on how to use BYOD safely, and this framework is updated periodically to enhance it.

The BYOD framework is referred to as lightweight as it does not involve expensive security products or systems, and it does not involve controlling student devices. Rather, it can be implemented through techniques such as conducting surveys among students, providing guidelines, awareness programs, MFA, updates, Wi-Fi security, and backups.

Framework Components

Table 7. Framework Components

Component	Purpose	Example Activity	Related BYOD Risk Addressed
Identity	Understand student BYOD usage and risky behavior	Student survey, device usage analysis	Unknown BYOD usage patterns
Access	Understand student BYOD usage and risky behavior	Risk matrix and scoring table	Password reuse, no MFA, public Wi-Fi
Govern	Define rules, responsibilities, and minimum security expectations	BYOD policy and acceptable use guidelines	Lack of formal BYOD control
Protect	Apply practical security controls	MFA, strong passwords, updates, antivirus, backup	Credential theft, malware, data loss
Educate	Improve student cybersecurity awareness	Awareness sessions, posters, and email reminders	Phishing, unsafe Wi-Fi, and poor password habits
Review	Continuously improve BYOD risk management	Semester-based review and repeated survey	Changing student behavior and new risks

Source: Developed from primary survey data collected for this study

1. Identify phase forms the initial step of the framework. At this phase, the university obtains information on how students use personal devices to engage in their studies. This includes what kind of devices students use, the types of services they access, and their usual security practices. The identify phase was facilitated by conducting surveys among 74 university students.
2. Assess will translate behavioral actions into risk scores. Risks in this study were measured using the likelihood and impact methodology. For instance, the reuse of passwords was considered a high risk, as a password breach may result in several other passwords being affected. Public Wi-Fi access was also categorized as a high risk due to its prevalence among students for accessing educational services
3. Governance revolves around policies and responsibilities. Institutions can establish guidelines on how students should use their own devices at universities through BYOD. For example, students should be instructed to use strong passwords, enable multifactor

authentication, update their devices regularly, avoid insecure networks, and protect institution-specific data. However, the institution will not completely govern the students' devices.

4. Protection consists of controls that mitigate the risks identified earlier. These controls must be easy and feasible to apply. Some examples of such controls are enabling multi-factor authentication, strong password usage, system software updates, installation of antivirus software, enabling screen locks, and backing up school-related documents.
5. Education is critical since most of the risks associated with BYOD are related to user practices. It is essential for students to be aware of the dangers of password reuse, suspicious links, public Wi-Fi, and a lack of backups. These awareness campaigns can be conducted via training sessions, posters, LMS announcements, email campaigns, or orientations.
6. The Review step guarantees that BYOD governance will not be considered just a one-off task. Student conduct, cyber risks, and technologies used at school may evolve over time. This is why the university needs to review the associated risks on a regular basis, ideally once per semester. This can help the university continuously improve its BYOD security strategy.

Mapping with NIST CSF 2.0

Table 8 below demonstrates that the proposed L-BGRF model can be aligned with the core principles of cybersecurity governance according to NIST CSF 2.0 (National Institute of Standards and Technology, 2024). The Govern component can be realized through policies on BYOD, assigning responsibility, and risk management. This is critical since the BYOD issue is not merely a technological challenge but requires institution-based policy and student responsibilities.

The identifying component can be achieved by analyzing how students use their devices and through risk identification surveys. In this study, risks related to password reuse, absence of MFA, public Wi-Fi use, non-routine updates, and backup were revealed by conducting a survey.

The assessment step allows for achieving the goals of both components—Governing and Identifying. It helps understand the university's priorities concerning existing threats, as it turned out that risks related to password reuse, the absence of MFA, and public Wi-Fi use deserve special attention.

Table 8. Mapping with NIST CSF 2.0

L-BGRF Component	Related NIST CSF 2.0 Function
Govern	Govern
Identify	Identify
Protect	Protect
Educate	Govern/Protect
Review	Detect/Respond/Recover

Source: Developed from primary survey data collected for this study

The Protect element uses actual controls, like using a good password, MFA, software update, antivirus, secure cloud, screen lock, and backup as its controls, which would make it easier to mitigate some of the risks that exist in relation to BYOD. The element Educate is used for governance and protection purposes because awareness is needed in order for the student to implement good security practices. The lack of awareness means that the policy will be useless. The Review element enables continuous improvement. Through this, the university will be able to observe any changes in student behavior and refine the BYOD risk matrix.

ISO/IEC 27001-Inspired Controls

The ISO/IEC 27001-inspired controls (ISO, 2022) provide a practical security control layer for the proposed framework. Since ISO/IEC 27001 focuses on information security management, its principles can be adapted to the university BYOD context through simplified controls. The purpose is not to fully implement ISO/IEC 27001 certification, but to use its risk-based thinking to guide student BYOD security. The ISO/IEC 27001-inspired controls are shown in Table 9 below.

For access control, students should be encouraged to use strong, unique passwords, avoid password reuse, and enable MFA for university-related accounts. These controls directly address the high-risk findings related to password reuse and the lack of MFA. For device security, students should be guided to keep devices updated, use antivirus or built-in protection, enable screen locks, and avoid installing untrusted applications. These controls reduce the risk of malware infection, unauthorized access, and exploitation of known software vulnerabilities.

For data protection, students should be advised to store academic files securely, avoid careless file sharing, and maintain regular backups. This is important because BYOD devices often contain assignments, research documents, login sessions, downloaded files, and shared academic materials. To promote awareness and reporting, the university should provide simple guidance on phishing, suspicious links, public Wi-Fi risks, and incident reporting. Students should know what to do if they suspect their account or device has been compromised. A simple reporting method, such as contacting the IT helpdesk or using a university-provided form, can improve response and recovery.

Table 9. ISO/IEC 27001-inspired controls

BYOD Risk	Recommended Control
Weak password	Password policy and MFA
Lost device	Screen lock and device encryption
Malware	Antivirus and software updates
Phishing	Awareness training
Data leakage	Secure cloud storage guidance
No backup	Backup recommendation
Unknown incidents	Reporting procedure

Source: Developed from primary survey data collected for this study

CONCLUSIONS

In this study, we evaluated the Bring-Your-Own-Device (BYOD) usage of university students and developed a lightweight governance and risk assessment framework (L-BGRF). The findings show that student-owned devices are commonly used for academic purposes. 55% of participants use only laptops for academic purposes, and 27% use both laptops and smartphones. This indicates increasing private access to communications and university resources and highlights the need for effective governance and risk management processes.

The analysis of password and authentication policies showed generally good security practices, with most students (81%) reporting the use of strong passwords or PINs and 76% employing multi-factor authentication. The reuse of passwords is still a significant problem, with 42% of respondents saying they use the same password for multiple accounts. Reusing passwords increases the likelihood of credential compromise and account takeover attacks and is a major cybersecurity concern in BYOD environments.

The results show that around 68% of the students keep their devices properly updated and use antivirus or security protection mechanisms. The survey also reaffirmed that all respondents lock their device screens. These results indicate a reasonable level of awareness of device security; however, a significant proportion of users still risk being infected with malware, facing software

vulnerabilities, and allowing unauthorized access to themselves and the university system.

The biggest security concerns are network and data security policies. The results show that 82% frequently use public Wi-Fi networks, which can leave sensitive and personal information vulnerable to cyberattacks if proper security measures are not put in place. Moreover, 79% of respondents said they do not regularly back up important academic data, increasing the risk of permanent data loss in the event of device failure, theft, or ransomware attacks. Cloud services, email, and online learning platforms are proliferating; while only 37% reported clicking on suspicious links, the reach of the threats posed by phishing attacks is growing.

The primary research problem was user practices and behaviors regarding the use of BYOD devices within higher education institutions. This risk assessment identified the highest risks associated with BYOD, such as the use of public Wi-Fi, lack of proper backup practices, password reuse, and some users not using multi-factor authentication. These findings confirm that technological cybersecurity challenges in university environments are affected not only by user behavior, but also by awareness levels and governance practices. The paper proposes the Lightweight BYOD Governance and Risk Framework (L-BGRF) to address these challenges, which integrates six key phases: Identify, Assess, Control, Protect, Educate, and Review. The framework gives universities a practical and cost-effective way to identify risks associated with BYOD, implement appropriate security controls, improve cybersecurity awareness, and continuously monitor risk levels.

LIMITATION & FURTHER RESEARCH

In addition, there are some limitations in this study. First, the sample size was small because the study was conducted within a short period and used only 100 university undergraduates. In future research, the student count will increase considerably, drawing from not only the from Kelaniya university but also from other universities. Second, because of the self-reported survey responses, this study may not completely represent actual student behavior. For further research, behavioral data will be collected using system logs, LMS activities, email activities, and simulated phishing exercises. Third, the proposed framework was evaluated conceptually and on the basis of survey-based findings, rather than through long-term institutional implementation. In future research, the study will be implemented in other universities.

REFERENCES

Abdul Halim, I. I., Buja, A. G., Mohamad Zain, J., Ngah, A. H., & Bansal, R. (2024). BYOD security policy model: A systematic literature review. *Journal of Advanced Research in Applied Sciences and Engineering Technology, 62*(1), 170–186. https://doi.org/10.37934/araset.62.1.170186

Ajmal, I. (2026). *Cybersecurity awareness and online safety practices among university students* [Bachelor's thesis, Metropolia University of Applied Sciences]. Theseus. https://urn.fi/URN:NBN:fi:amk-202603315394

Akampurira, P., Edozie, E., Olaniyi Sadiq, B., & Dahiru Buhari, M. (2026). A deep learning-based user behavior analytics model for proactive cyber threat detection and risk management: A review. *F1000Research, 15*, 674. https://doi.org/10.12688/f1000research.178351.1

Alghabban, W. G. (2026). ZeroTrustEdu: A lightweight post-quantum cryptography framework with adaptive trust scoring for secure cloud-IoT e-learning platforms. *Electronics, 15*(10), 2132. https://doi.org/10.3390/electronics15102132

Ali, M. G. (2025). *Cybersecurity governance and policy development in higher education institutions: A strategic framework for resilience and compliance*. ERIC. https://eric.ed.gov/?id=ED675147

Almarhabi, K., Jambi, K., Eassa, F., & Batarfi, O. (2018). An evaluation of the proposed framework for access control in the cloud and BYOD environment. *International Journal of Advanced*

Computer Science and Applications, 9(10), 213–221. https://doi.org/10.14569/IJACSA.2018.091026

Althobaiti, K., & Alsufyani, N. (2024). A review of organization-oriented phishing research. *PeerJ Computer Science, 10*, e2487. https://doi.org/10.7717/peerj-cs.2487

Barruga, M. B. (2025). Systematic review of cybersecurity frameworks for higher education institutions: Characteristics, components, and challenges. *International Journal of Applied Mathematics, 38*(4).

Batalla, G. A., Fernando, R. A., Arcillas, M., Cerdeña, J., Castillo, J. G., Barcenal, A. L., Batalla, G., Tolentino, A., Malitig, F., & Barrion, L. O. (2026). Support staff performance and client satisfaction-based office productivity in higher education: A descriptive-correlational study. *Applied Quantitative Analysis, 6*(1), 59–75. https://doi.org/10.31098/quant.4337

Bottyan, L. (2023). Cybersecurity awareness among university students. *Journal of Applied Technical and Educational Sciences, 13*(3). https://doi.org/10.24368/JATES363

Bwiino, K., Mayoka, G. K., Nkamwesiga, L., & Nyamadi, M. (2026). A systematic literature review of information security practices in higher education contexts. *IET Information Security, 2026*(1), 6324508. https://doi.org/10.1049/ise2/6324508

Dawaare, B. (2025). *A risk evaluation framework and comprehensive security compliance assessment solution for space information networks (SIN)* [Master's thesis, Dakota State University]. Dakota State University. https://scholar.dsu.edu/theses/481

De La Torre, R. E., Jr., Andrada, H. G., Catador, J. J. C., Tan, C., Pantonial, M. J., & Panaga, D. (2026). INSIGHT: Improving numeracy skills on integers through e-games and hands-on technology. *Advanced Journal of STEM Education, 4*(1), 1–15. https://doi.org/10.31098/ajosed.v4i1.3180

Dina, M. (2025). Security vulnerabilities in South African higher education LMSs: Evaluating the risks of BYOD integration. In *Proceedings of the 2025 International Conference on Artificial Intelligence, Big Data, Computing and Data Communication Systems* (pp. 1–7). https://doi.org/10.1145/3759023.3759099

Essahraui, S., Lamaakal, I., Maleh, Y., El Makkaoui, K., Filali Bouami, M., Ouahbi, I., Abd El-Latif, A. A., Almousa, M., & Rodrigues, J. J. P. C. (2025). Human behavior analysis: A comprehensive survey on techniques, applications, challenges, and future directions. *IEEE Access, 13*, 128379–128419. https://doi.org/10.1109/ACCESS.2025.3589938

Handri, M. A., Abdullah, F. A., & Nawal, H. N. (2026). The dominance of market expectations over systematic risk on stock prices: Evidence from fixed-effects panel regression in Indonesia's LQ45 manufacturing sector. *Applied Quantitative Analysis, 6*(1), 44–58. https://doi.org/10.31098/quant.4116

Harthy, K. A. (2022). *A risk management framework for the BYOD environment*.

Hassan, A., Rauf, A., Shafqat, N., Latif, R., & Khan, H. (2025). ZenGuard: A machine learning-based zero trust framework for context-aware threat mitigation using SIEM, SOAR and UEBA. *Scientific Reports, 15*(1), 35871. https://doi.org/10.1038/s41598-025-20998-4

International Organization for Standardization. (2022). *Information security, cybersecurity and privacy protection—Information security management systems—Requirements (ISO/IEC Standard No. 27001:2022).* https://www.iso.org/standard/27001

Kepuska, K., & Tomasevic, M. (2024). A lightweight framework for cyber risk management in Western Balkan higher education institutions. *PeerJ Computer Science, 10*, e1958. https://doi.org/10.7717/peerj-cs.1958

Moeti, W., Moyo, S., & Moropana, T. (2025). *Compliance and internal controls: Standards and practices in cyber security governance* (SSRN Scholarly Paper No. 5581811). Social Science Research Network. https://doi.org/10.2139/ssrn.5581811

National Institute of Standards and Technology. (2024). *The NIST cybersecurity framework (CSF) 2.0*

(NIST CSWP 29). U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.29

Osijirin, A. N., Anigbo, L. C., Okechukwu, O., Okporie, C., Agwuama, & Sada, S. M. (2026). Cybersecurity and digital learning in higher education: Emerging threats, protective technologies, and future directions. *Asian Journal of Research in Computer Science, 19*(7), 137–155. https://doi.org/10.9734/ajrcos/2026/v19i7884

Soni, A., Kumar Nanda, S., Priyadarshini, R., & Panda, G. (2026). A comprehensive review and comparative analysis of zero trust architecture: Evolution, implementation strategies, and key challenges. *Journal of Computer Security, 34*(2), 85–110. https://doi.org/10.1177/0926227X251409922

Vasović, D., Janaćković, G., Vranjanac, Ž., Stamenković, S., & Vasović, B. (2026). Enhancing CIA triad—Confidentiality, integrity and availability in educational information systems through next-generation ISO/IEC 27001:2022-aligned security model. *Applied Sciences, 16*(12), 6260. https://doi.org/10.3390/app16126260

Weeratunge, N. H., Hjelsvold, R., & Katt, B. (2026). A systematic scoping review on game-based cybersecurity awareness education. *International Journal of Information Security, 25*(2), 71. https://doi.org/10.1007/s10207-026-01239-9

Whitman, M. E., & Mattord, H. J. (2021). *Principles of information security* (7th ed.). Cengage Learning.

Yaakub, N. A. M., Sumin, V., & Ling, U. L. (2026). Agriculture IoT adoption: Linking technology readiness, acceptance and entrepreneurial ambidexterity among Sabah smallholders. *Applied Quantitative Analysis, 6*(1), 89–115. https://doi.org/10.31098/quant.4115

Zentner, A., & West, T. (2026). *Shadow AI in higher education: A socio-technical framework for governing unauthorized employee use of artificial intelligence* (SSRN Scholarly Paper No. 7051078). Social Science Research Network. https://doi.org/10.2139/ssrn.7051078